LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 6
PEMBACAAN LOG SERVER

Disusun oleh :

Nama	: Aura Nisa’ Hidayat
NIM	: 21/482690/SV/19983
Kelas	: TRI A
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Hari, Tanggal	: Selasa, 7 Maret 2023

PROGRAM STUDI DIV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Laporan Praktikum Kamanan Informasi 1

Unit 6: Pembacaan Log Server

I. TUJUAN

- Membaca file log dengan *cat*, *more*, *less,* dan *tail*
- Memahami file log dan syslog
- Memahami file log dan jurnalctl

II. LATAR BELAKANG

File Log adalah alat penting dalam pemecahan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar sama. Di lab ini, Anda akan mempelajari tentang alat umum yang digunakan untuk membaca file log dan berlatih menggunakannya. Log server adalah file log yang dibuat dan dipelihara oleh server secara otomatis. Peringatan berisi daftar aktivitas yang dilakukan server, seperti jumlah permintaan halaman, alamat IP klien, jenis permintaan, dan lain sebagainya. File log memiliki fungsi untuk mengidentifikasi dan memecahkan masalah kesalahan, meningkatkan operasi, meningkatkan efisiensi, memahami perilaku pengguna, dan memperkuat keamanan.

Syslog merupakan sebuah singkatan dari kata *System Logging Protocol* yang merupakan protokol standar yang dapat digunakan untuk mengirim log sistem atau pesan peristiwa ke server tertentu. Semua pesan syslog mengikuti format standar yang diperlukan untuk bertukar pesan antar aplikasi. Format ini mencakup komponen berikut: Header yang berisi bidang khusus untuk prioritas, versi, stempel waktu, nama host, aplikasi, ID proses, dan ID pesan. Log Linux dapat dilihat menggunakan perintah cd /var/log, kemudian jalankan perintah ls untuk melihat log yang disimpan di direktori tersebut. Salah satu log terpenting adalah syslog, yang mencatat semuanya kecuali pesan terkait auth.

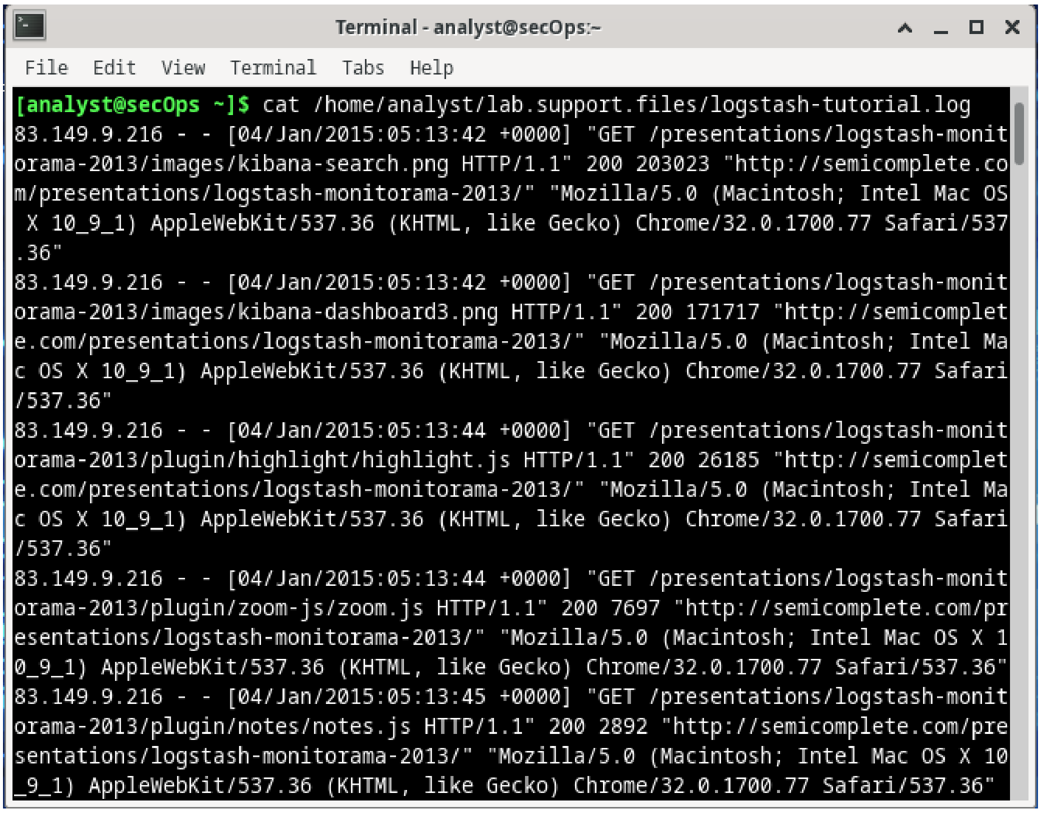
III. ALAT DAN BAHAN

- CyberOps workstation virtual machine

IV. INSTRUKSI KERJA

1. Langkah pertama adalah membuka VM CyberOps Worstation dan jendala terminal.

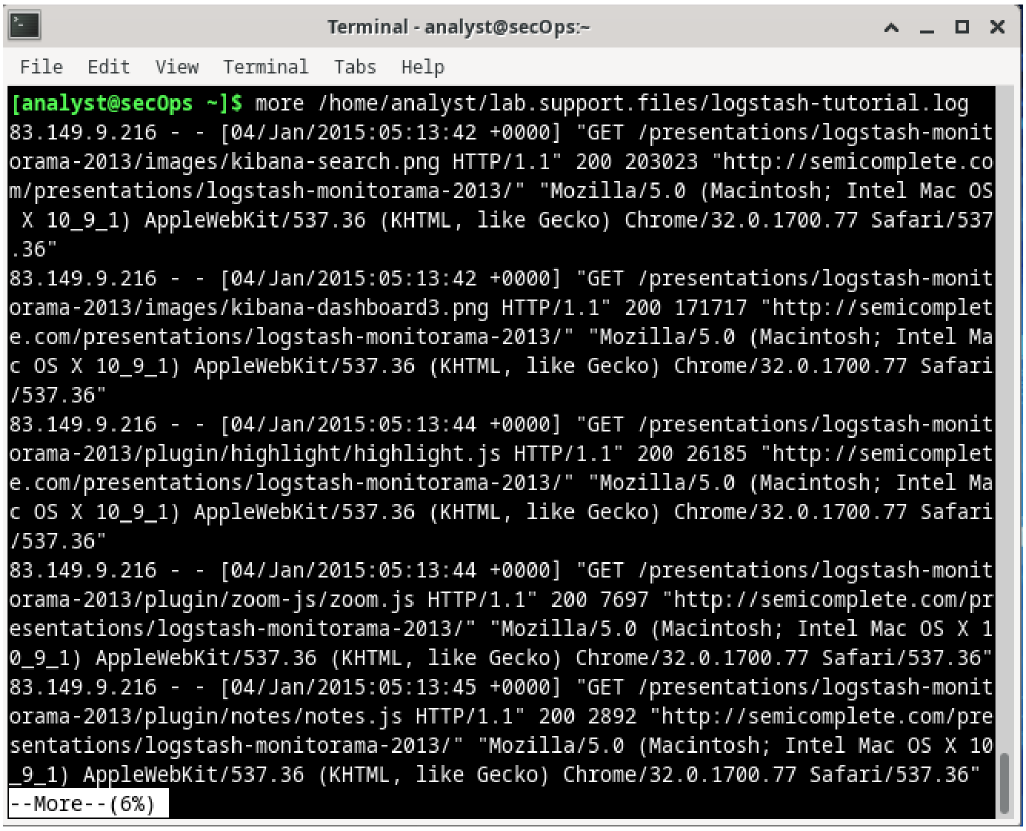
2. Dari jendela terminal, jalankan perintah di bawah ini untuk menampilkan konten file logstash-tutorial.log, yang terletak di folder /home/analyst/lab.support.files/:
   analis@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log



Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ cat /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
 X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
```

3. Dari jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more: analis@secOps ~$ more /home/analyst/lab.support.files/logstash-tutorial.log

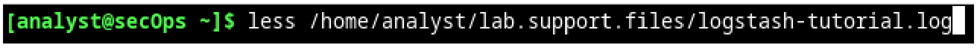


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

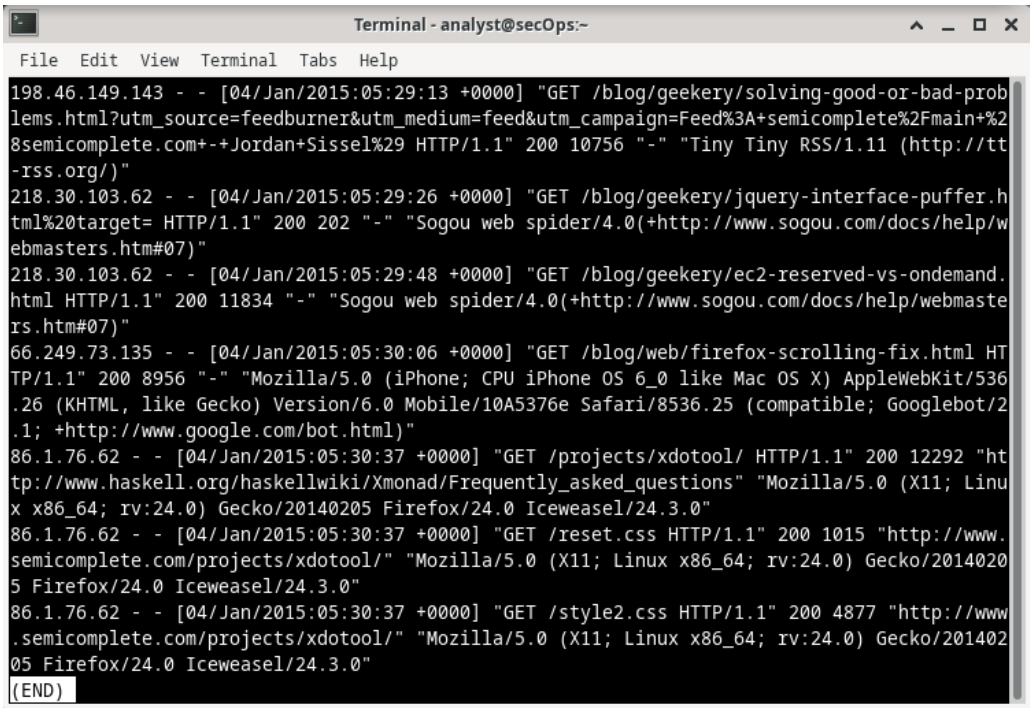
```
[analyst@secOps ~]$ more /home/analyst/lab.support.files/logstash-tutorial.log
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS
 X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537
.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari
/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10
_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
--More--(6%)
```

4. Dari tampilan terminal yang sama, gunakan less untuk menampilkan konten file logstashtutorial.log lagi:

   analis@secOps ~$ lebih sedikit /home/analyst/lab.support.files/logstash-tutorial.log



```
[analyst@secOps ~]$ less /home/analyst/lab.support.files/logstash-tutorial.log
```



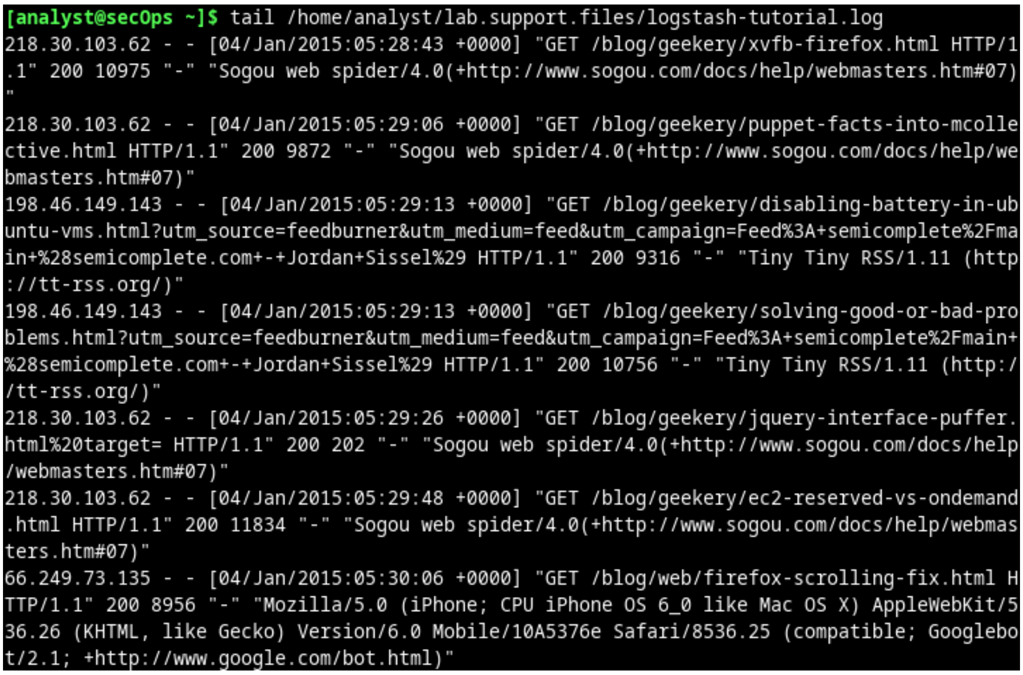
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-prob
lems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%2
8semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt
-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.h
tml%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/w
ebmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.
html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmaste
rs.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html HT
TP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536
.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2
.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "ht
tp://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linu
x x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /reset.css HTTP/1.1" 200 1015 "http://www.
semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/2014020
5 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /style2.css HTTP/1.1" 200 4877 "http://www
.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/201402
05 Firefox/24.0 Iceweasel/24.3.0"
(END)
```

5. Perintah tail menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file. Gunakan tail untuk menampilkan sepuluh baris terakhir dari file /home/analyst/lab.support.files/logstash-tutorial.log

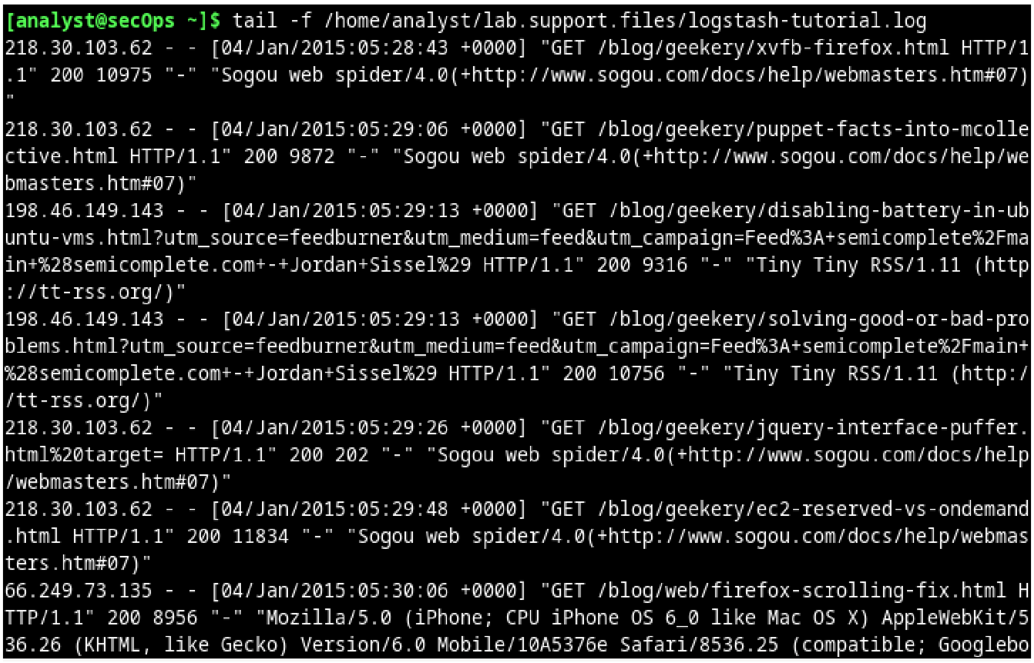
   analis@secOps ~$ tail /home/analyst/lab.support.files/logstash-tutorial.log

   tail

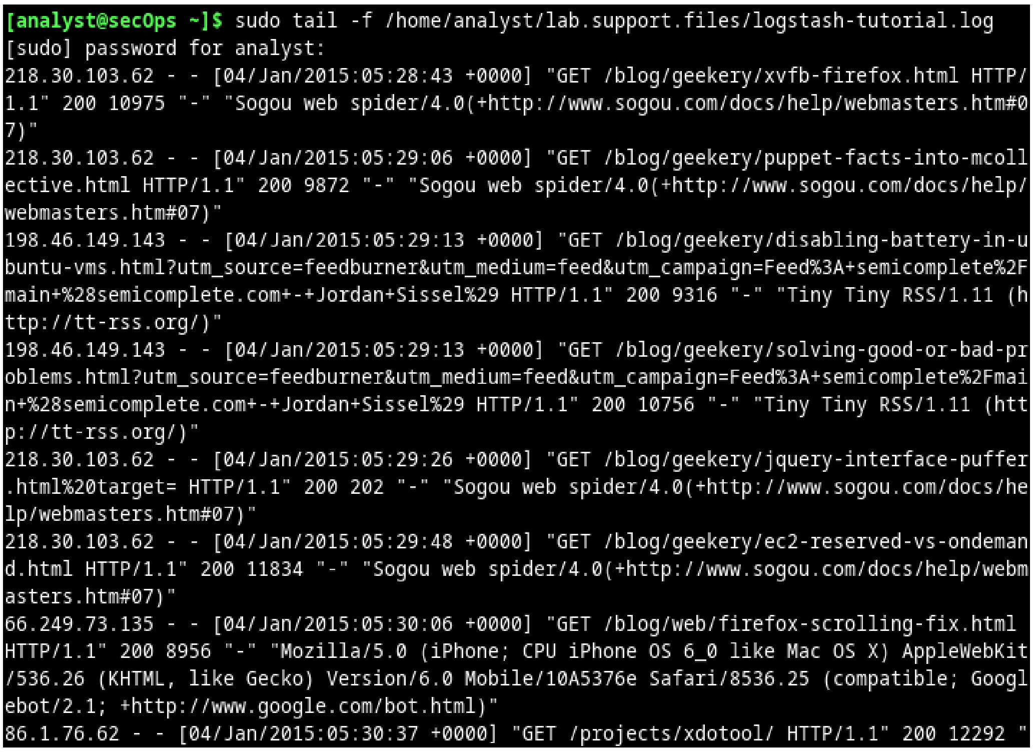


```
[analyst@secOps ~]$ tail /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1
.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)
"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcolle
ctive.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/we
bmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ub
untu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fma
in+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http
://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-pro
blems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+
%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http:/
/tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.
html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help
/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand
.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmas
ters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html H
TTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/5
36.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebo
t/2.1; +http://www.google.com/bot.html)"
```

tail -f



```
[analyst@secOps ~]$ tail -f /home/analyst/lab.support.files/logstash-tutorial.log
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/1
.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)
"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcolle
ctive.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/we
bmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-ub
untu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fma
in+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http
://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-pro
blems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+
%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http:/
/tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.
html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help
/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand
.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmas
ters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html H
TTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/5
36.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebo
```

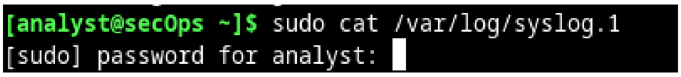


```
[analyst@secOps ~]$ sudo tail -f /home/analyst/lab.support.files/logstash-tutorial.log
[sudo] password for analyst:
218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "GET /blog/geekery/xvfb-firefox.html HTTP/
1.1" 200 10975 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#0
7)"
218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcoll
ective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/
webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/disabling-battery-in-u
buntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2F
main+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (h
ttp://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-pr
oblems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmai
n+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (htt
p://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer
.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/he
lp/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondeman
d.html HTTP/1.1" 200 11834 "-" "Sogou web spider/4.0(+http://www.sogou.com/docs/help/webm
asters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "GET /blog/web/firefox-scrolling-fix.html
HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit
/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googl
ebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "
```

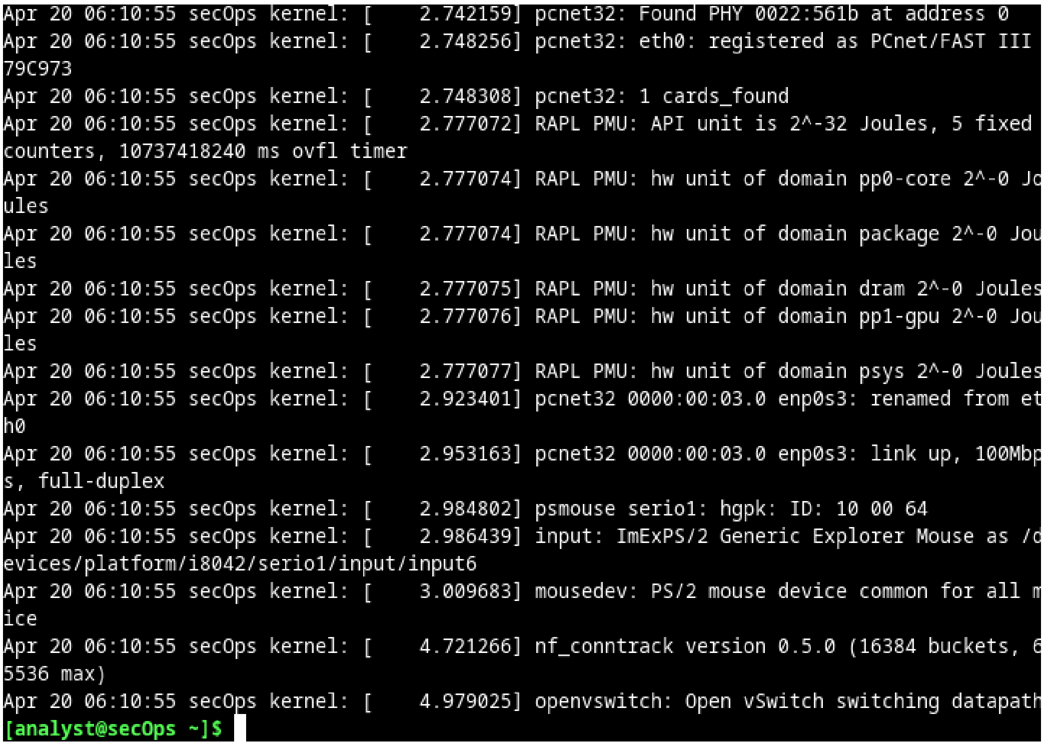
6. Pilihlah jendela terminal bawah dan masukkan perintah berikut:
   [analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log

7. Gunakan perintah cat sebagai root untuk membuat daftar isi file /var/log/syslog.1. File ini menyimpan entri log yang dihasilkan oleh sistem operasi CyberOps Workstation VM dan dikirim ke layanan syslog.

analis@secOps ~$ sudo cat /var/log/syslog.1



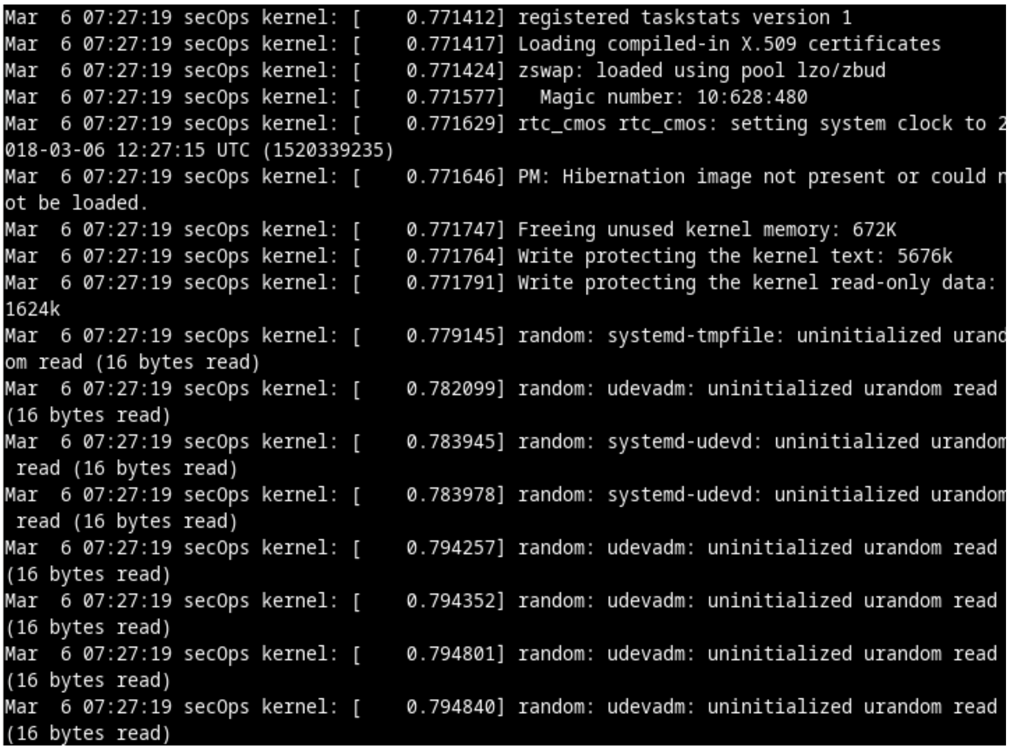
```
[analyst@secOps ~]$ sudo cat /var/log/syslog.1
[sudo] password for analyst:
```



```
Apr 20 06:10:55 secOps kernel: [    2.742159] pcnet32: Found PHY 0022:561b at address 0
Apr 20 06:10:55 secOps kernel: [    2.748256] pcnet32: eth0: registered as PCnet/FAST III
79C973
Apr 20 06:10:55 secOps kernel: [    2.748308] pcnet32: 1 cards_found
Apr 20 06:10:55 secOps kernel: [    2.777072] RAPL PMU: API unit is 2^-32 Joules, 5 fixed
counters, 10737418240 ms ovfl timer
Apr 20 06:10:55 secOps kernel: [    2.777074] RAPL PMU: hw unit of domain pp0-core 2^-0 Jo
ules
Apr 20 06:10:55 secOps kernel: [    2.777074] RAPL PMU: hw unit of domain package 2^-0 Jou
les
Apr 20 06:10:55 secOps kernel: [    2.777075] RAPL PMU: hw unit of domain dram 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.777076] RAPL PMU: hw unit of domain pp1-gpu 2^-0 Jou
les
Apr 20 06:10:55 secOps kernel: [    2.777077] RAPL PMU: hw unit of domain psys 2^-0 Joules
Apr 20 06:10:55 secOps kernel: [    2.923401] pcnet32 0000:00:03.0 enp0s3: renamed from et
h0
Apr 20 06:10:55 secOps kernel: [    2.953163] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbp
s, full-duplex
Apr 20 06:10:55 secOps kernel: [    2.984802] psmouse serio1: hgpk: ID: 10 00 64
Apr 20 06:10:55 secOps kernel: [    2.986439] input: ImExPS/2 Generic Explorer Mouse as /d
evices/platform/i8042/serio1/input/input6
Apr 20 06:10:55 secOps kernel: [    3.009683] mousedev: PS/2 mouse device common for all m
ice
Apr 20 06:10:55 secOps kernel: [    4.721266] nf_conntrack version 0.5.0 (16384 buckets, 6
5536 max)
Apr 20 06:10:55 secOps kernel: [    4.979025] openvswitch: Open vSwitch switching datapath
[analyst@secOps ~]$
```

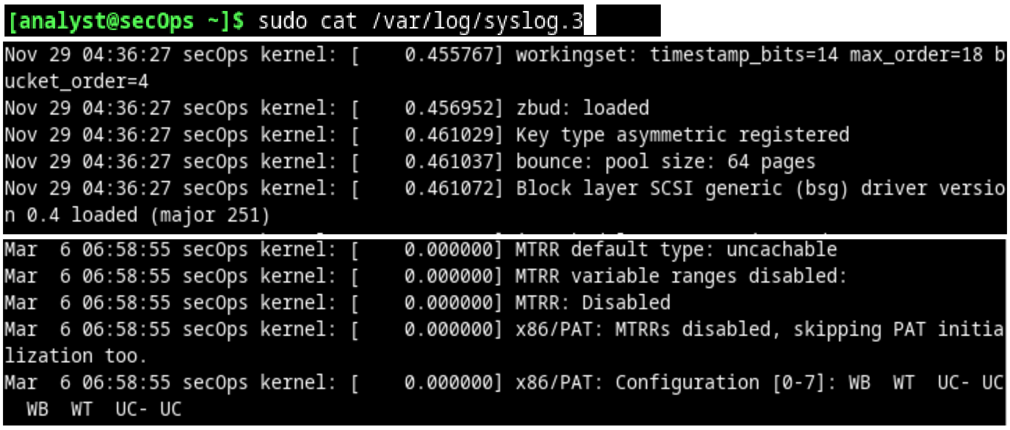
8. Mengganti nama file log lama menjadi syslog.1, syslog.2, dan seterusnya. Gunakan perintah cat untuk membuat daftar file syslog yang lebih lama:
   analis@secOps ~$ sudo cat /var/log/syslog.2

```
[analyst@secOps ~]$ sudo cat /var/log/syslog.2
```



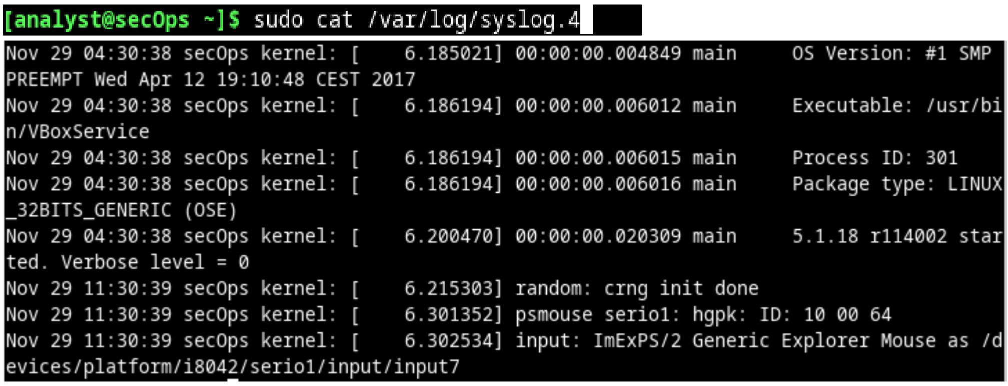
```
Mar  6 07:27:19 secOps kernel: [    0.771412] registered taskstats version 1
Mar  6 07:27:19 secOps kernel: [    0.771417] Loading compiled-in X.509 certificates
Mar  6 07:27:19 secOps kernel: [    0.771424] zswap: loaded using pool lzo/zbud
Mar  6 07:27:19 secOps kernel: [    0.771577]   Magic number: 10:628:480
Mar  6 07:27:19 secOps kernel: [    0.771629] rtc_cmos rtc_cmos: setting system clock to 2
018-03-06 12:27:15 UTC (1520339235)
Mar  6 07:27:19 secOps kernel: [    0.771646] PM: Hibernation image not present or could n
ot be loaded.
Mar  6 07:27:19 secOps kernel: [    0.771747] Freeing unused kernel memory: 672K
Mar  6 07:27:19 secOps kernel: [    0.771764] Write protecting the kernel text: 5676k
Mar  6 07:27:19 secOps kernel: [    0.771791] Write protecting the kernel read-only data:
1624k
Mar  6 07:27:19 secOps kernel: [    0.779145] random: systemd-tmpfile: uninitialized urand
om read (16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.782099] random: udevadm: uninitialized urandom read
(16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.783945] random: systemd-udevd: uninitialized urandom
 read (16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.783978] random: systemd-udevd: uninitialized urandom
 read (16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.794257] random: udevadm: uninitialized urandom read
(16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.794352] random: udevadm: uninitialized urandom read
(16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.794801] random: udevadm: uninitialized urandom read
(16 bytes read)
Mar  6 07:27:19 secOps kernel: [    0.794840] random: udevadm: uninitialized urandom read
(16 bytes read)
```

analis@secOps ~$ sudo cat /var/log/syslog.3



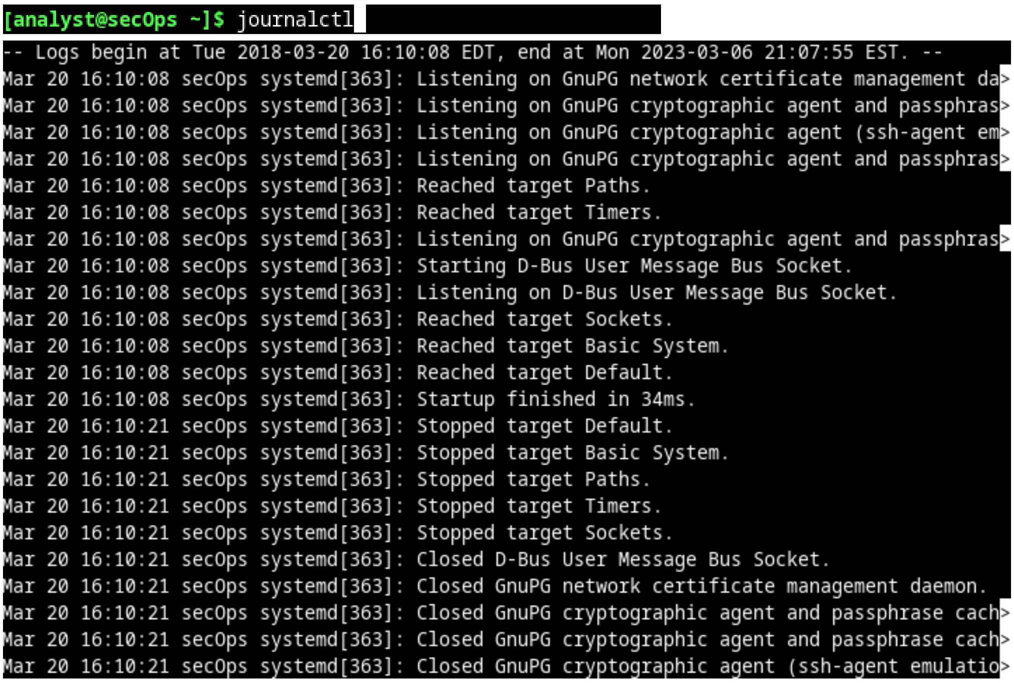
```
[analyst@secOps ~]$ sudo cat /var/log/syslog.3
Nov 29 04:36:27 secOps kernel: [    0.455767] workingset: timestamp_bits=14 max_order=18 b
ucket_order=4
Nov 29 04:36:27 secOps kernel: [    0.456952] zbud: loaded
Nov 29 04:36:27 secOps kernel: [    0.461029] Key type asymmetric registered
Nov 29 04:36:27 secOps kernel: [    0.461037] bounce: pool size: 64 pages
Nov 29 04:36:27 secOps kernel: [    0.461072] Block layer SCSI generic (bsg) driver versio
n 0.4 loaded (major 251)
Mar  6 06:58:55 secOps kernel: [    0.000000] MTRR default type: uncachable
Mar  6 06:58:55 secOps kernel: [    0.000000] MTRR variable ranges disabled:
Mar  6 06:58:55 secOps kernel: [    0.000000] MTRR: Disabled
Mar  6 06:58:55 secOps kernel: [    0.000000] x86/PAT: MTRRs disabled, skipping PAT initia
lization too.
Mar  6 06:58:55 secOps kernel: [    0.000000] x86/PAT: Configuration [0-7]: WB  WT  UC- UC
  WB  WT  UC- UC
```

analis@secOps ~$ sudo cat /var/log/syslog.4

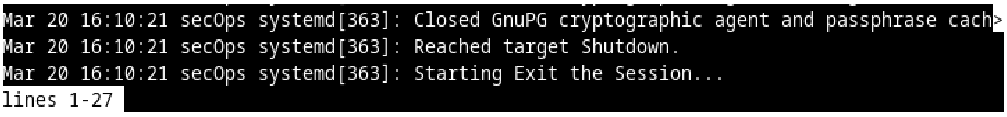


```
[analyst@secOps ~]$ sudo cat /var/log/syslog.4
Nov 29 04:30:38 secOps kernel: [    6.185021] 00:00:00.004849 main     OS Version: #1 SMP
PREEMPT Wed Apr 12 19:10:48 CEST 2017
Nov 29 04:30:38 secOps kernel: [    6.186194] 00:00:00.006012 main     Executable: /usr/bi
n/VBoxService
Nov 29 04:30:38 secOps kernel: [    6.186194] 00:00:00.006015 main     Process ID: 301
Nov 29 04:30:38 secOps kernel: [    6.186194] 00:00:00.006016 main     Package type: LINUX
_32BITS_GENERIC (OSE)
Nov 29 04:30:38 secOps kernel: [    6.200470] 00:00:00.020309 main     5.1.18 r114002 star
ted. Verbose level = 0
Nov 29 11:30:39 secOps kernel: [    6.215303] random: crng init done
Nov 29 11:30:39 secOps kernel: [    6.301352] psmouse serio1: hgpk: ID: 10 00 64
Nov 29 11:30:39 secOps kernel: [    6.302534] input: ImExPS/2 Generic Explorer Mouse as /d
evices/platform/i8042/serio1/input/input7
```

9. Memahami File Log dan Jurnalctl, untuk melihat log journald, gunakan perintah journalctl. Alat journalctl menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal.
analis@secOps ~$ journalctl



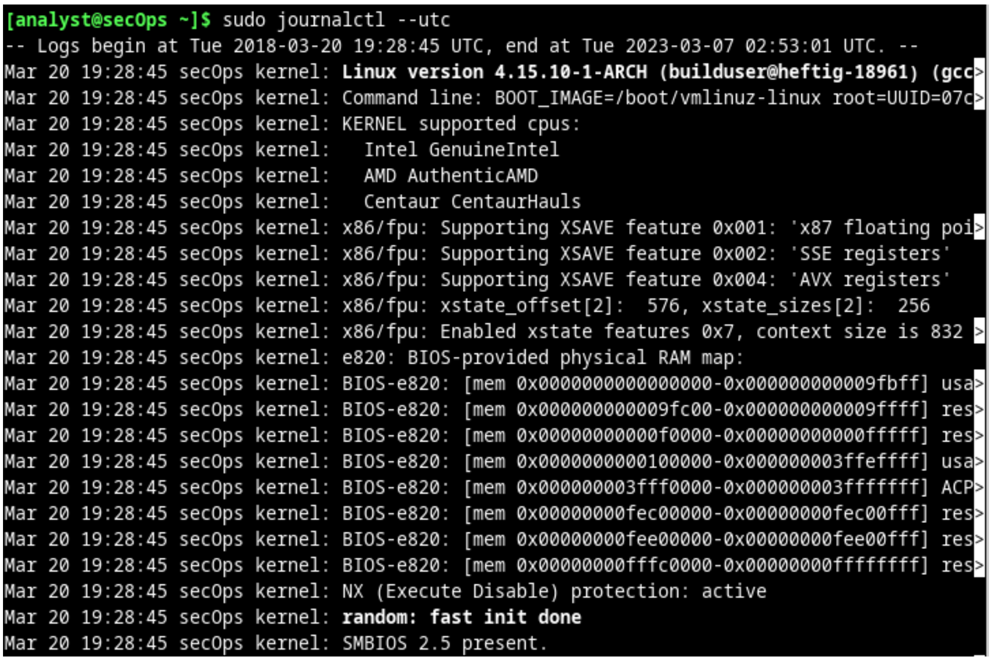
```
[analyst@secOps ~]$ journalctl
-- Logs begin at Tue 2018-03-20 16:10:08 EDT, end at Mon 2023-03-06 21:07:55 EST. --
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG network certificate management da>
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphras>
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent (ssh-agent em>
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphras>
Mar 20 16:10:08 secOps systemd[363]: Reached target Paths.
Mar 20 16:10:08 secOps systemd[363]: Reached target Timers.
Mar 20 16:10:08 secOps systemd[363]: Listening on GnuPG cryptographic agent and passphras>
Mar 20 16:10:08 secOps systemd[363]: Starting D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Listening on D-Bus User Message Bus Socket.
Mar 20 16:10:08 secOps systemd[363]: Reached target Sockets.
Mar 20 16:10:08 secOps systemd[363]: Reached target Basic System.
Mar 20 16:10:08 secOps systemd[363]: Reached target Default.
Mar 20 16:10:08 secOps systemd[363]: Startup finished in 34ms.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Default.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Basic System.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Paths.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Timers.
Mar 20 16:10:21 secOps systemd[363]: Stopped target Sockets.
Mar 20 16:10:21 secOps systemd[363]: Closed D-Bus User Message Bus Socket.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG network certificate management daemon.
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cach>
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cach>
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent (ssh-agent emulatio>
```



```
Mar 20 16:10:21 secOps systemd[363]: Closed GnuPG cryptographic agent and passphrase cach>
Mar 20 16:10:21 secOps systemd[363]: Reached target Shutdown.
Mar 20 16:10:21 secOps systemd[363]: Starting Exit the Session...
lines 1-27
```

Gunakan journalctl - -utc untuk menampilkan semua cap waktu dalam waktu UTC:

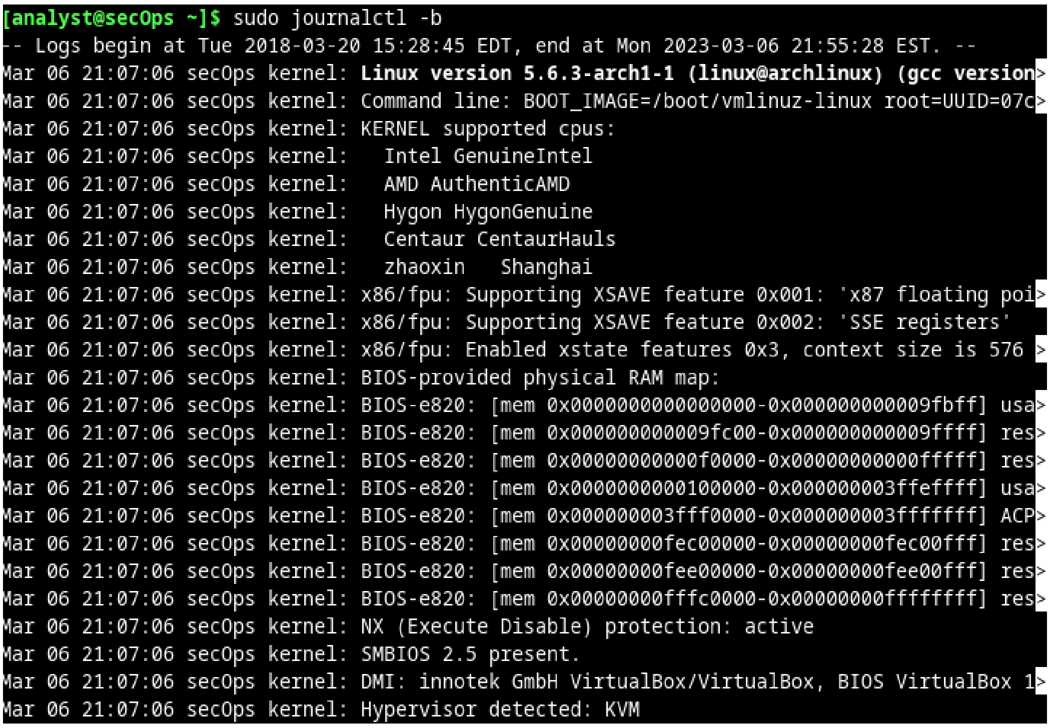
analis@secOps ~$ sudo journalctl --utc



```
[analyst@secOps ~]$ sudo journalctl --utc
-- Logs begin at Tue 2018-03-20 19:28:45 UTC, end at Tue 2023-03-07 02:53:01 UTC. --
Mar 20 19:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc>
Mar 20 19:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c>
Mar 20 19:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 19:28:45 secOps kernel:   Intel GenuineIntel
Mar 20 19:28:45 secOps kernel:   AMD AuthenticAMD
Mar 20 19:28:45 secOps kernel:   Centaur CentaurHauls
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating poi>
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 19:28:45 secOps kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Mar 20 19:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 >
Mar 20 19:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usa>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] res>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] res>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usa>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACP>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] res>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] res>
Mar 20 19:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] res>
Mar 20 19:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 19:28:45 secOps kernel: random: fast init done
Mar 20 19:28:45 secOps kernel: SMBIOS 2.5 present.
```

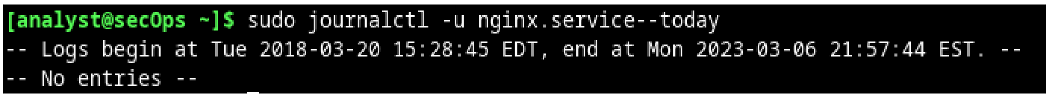
Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir:

analis@secOps ~$ sudo journalctl –b



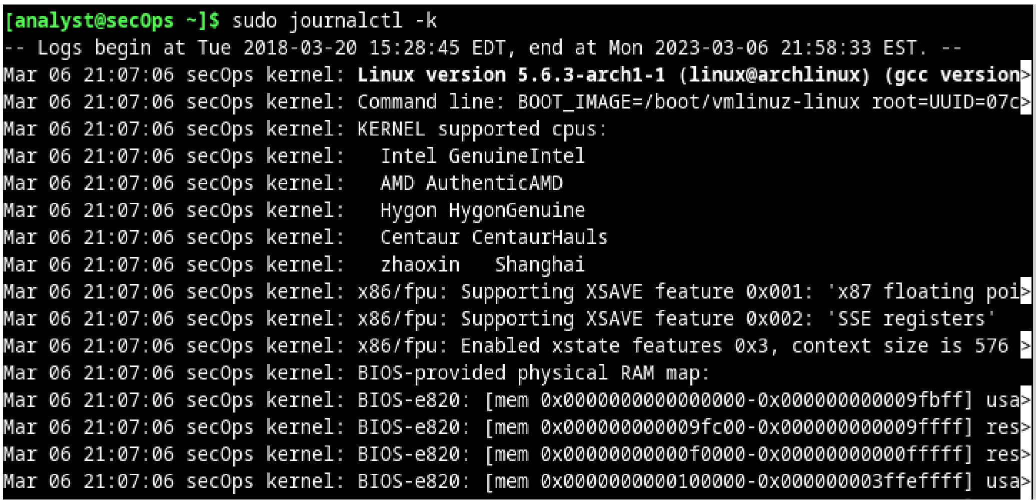
```
[analyst@secOps ~]$ sudo journalctl -b
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:55:28 EST. --
Mar 06 21:07:06 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version>
Mar 06 21:07:06 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c>
Mar 06 21:07:06 secOps kernel: KERNEL supported cpus:
Mar 06 21:07:06 secOps kernel:   Intel GenuineIntel
Mar 06 21:07:06 secOps kernel:   AMD AuthenticAMD
Mar 06 21:07:06 secOps kernel:   Hygon HygonGenuine
Mar 06 21:07:06 secOps kernel:   Centaur CentaurHauls
Mar 06 21:07:06 secOps kernel:   zhaoxin   Shanghai
Mar 06 21:07:06 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating poi>
Mar 06 21:07:06 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 21:07:06 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 >
Mar 06 21:07:06 secOps kernel: BIOS-provided physical RAM map:
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usa>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] res>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] res>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usa>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x000000003fff0000-0x000000003fffffff] ACP>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] res>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] res>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] res>
Mar 06 21:07:06 secOps kernel: NX (Execute Disable) protection: active
Mar 06 21:07:06 secOps kernel: SMBIOS 2.5 present.
Mar 06 21:07:06 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 1>
Mar 06 21:07:06 secOps kernel: Hypervisor detected: KVM
```

10. Gunakan journalctl untuk menentukan layanan dan kerangka waktu untuk entri log. Perintah di bawah ini menunjukkan semua log layanan nginx yang direkam hari ini: analis@secOps ~$ sudo journalctl -u nginx.service --sejak hari ini 12.



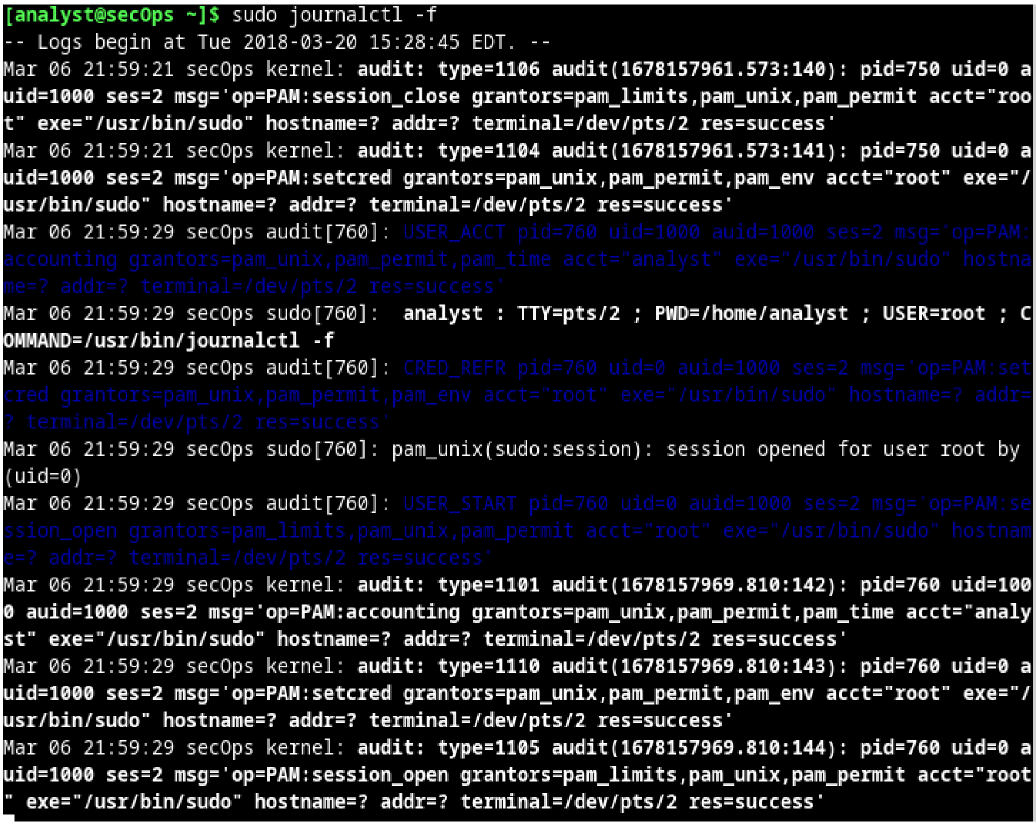
```
[analyst@secOps ~]$ sudo journalctl -u nginx.service--today
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:57:44 EST. --
-- No entries --
```

11. Gunakan sakelar -k untuk hanya menampilkan pesan yang dihasilkan oleh kernel: analis@secOps ~$ sudo journalctl –k 13. Mirip dengan tail -f yang dijelaskan di atas,



```
[analyst@secOps ~]$ sudo journalctl -k
-- Logs begin at Tue 2018-03-20 15:28:45 EDT, end at Mon 2023-03-06 21:58:33 EST. --
Mar 06 21:07:06 secOps kernel: Linux version 5.6.3-arch1-1 (linux@archlinux) (gcc version>
Mar 06 21:07:06 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c>
Mar 06 21:07:06 secOps kernel: KERNEL supported cpus:
Mar 06 21:07:06 secOps kernel:   Intel GenuineIntel
Mar 06 21:07:06 secOps kernel:   AMD AuthenticAMD
Mar 06 21:07:06 secOps kernel:   Hygon HygonGenuine
Mar 06 21:07:06 secOps kernel:   Centaur CentaurHauls
Mar 06 21:07:06 secOps kernel:   zhaoxin   Shanghai
Mar 06 21:07:06 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating poi>
Mar 06 21:07:06 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 06 21:07:06 secOps kernel: x86/fpu: Enabled xstate features 0x3, context size is 576 >
Mar 06 21:07:06 secOps kernel: BIOS-provided physical RAM map:
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usa>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] res>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] res>
Mar 06 21:07:06 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x000000003ffeffff] usa>
```

12. Gunakan -f untuk secara aktif mengikuti log saat sedang ditulis: analis@secOps ~$ sudo journalctl –f



```
[analyst@secOps ~]$ sudo journalctl -f
-- Logs begin at Tue 2018-03-20 15:28:45 EDT. --
Mar 06 21:59:21 secOps kernel: audit: type=1106 audit(1678157961.573:140): pid=750 uid=0 a
uid=1000 ses=2 msg='op=PAM:session_close grantors=pam_limits,pam_unix,pam_permit acct="roo
t" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 21:59:21 secOps kernel: audit: type=1104 audit(1678157961.573:141): pid=750 uid=0 a
uid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,pam_env acct="root" exe="/
usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 21:59:29 secOps audit[760]: USER_ACCT pid=760 uid=1000 auid=1000 ses=2 msg='op=PAM:
accounting grantors=pam_unix,pam_permit,pam_time acct="analyst" exe="/usr/bin/sudo" hostna
me=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 21:59:29 secOps sudo[760]:  analyst : TTY=pts/2 ; PWD=/home/analyst ; USER=root ; C
OMMAND=/usr/bin/journalctl -f
Mar 06 21:59:29 secOps audit[760]: CRED_REFR pid=760 uid=0 auid=1000 ses=2 msg='op=PAM:set
cred grantors=pam_unix,pam_permit,pam_env acct="root" exe="/usr/bin/sudo" hostname=? addr=
? terminal=/dev/pts/2 res=success'
Mar 06 21:59:29 secOps sudo[760]: pam_unix(sudo:session): session opened for user root by
(uid=0)
Mar 06 21:59:29 secOps audit[760]: USER_START pid=760 uid=0 auid=1000 ses=2 msg='op=PAM:se
ssion_open grantors=pam_limits,pam_unix,pam_permit acct="root" exe="/usr/bin/sudo" hostnam
e=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 21:59:29 secOps kernel: audit: type=1101 audit(1678157969.810:142): pid=760 uid=100
0 auid=1000 ses=2 msg='op=PAM:accounting grantors=pam_unix,pam_permit,pam_time acct="analy
st" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 21:59:29 secOps kernel: audit: type=1110 audit(1678157969.810:143): pid=760 uid=0 a
uid=1000 ses=2 msg='op=PAM:setcred grantors=pam_unix,pam_permit,pam_env acct="root" exe="/
usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
Mar 06 21:59:29 secOps kernel: audit: type=1105 audit(1678157969.810:144): pid=760 uid=0 a
uid=1000 ses=2 msg='op=PAM:session_open grantors=pam_limits,pam_unix,pam_permit acct="root
" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/2 res=success'
```

V. PEMBAHASAN

File log biasanya berisi informasi teks biasa yang dapat dilihat oleh hampir semua program yang dapat menangani teks. Namun, karena kemudahan, kegunaan, dan kecepatan, beberapa alat lebih umum digunakan daripada yang lain. Bagian ini berfokus pada empat program berbasis baris perintah cat, more, less, dan tail.

- Fitur ***cat***, berasal dari kata "*concatenate*", alat berbasis baris perintah yang digunakan untuk membaca dan menampilkan konten file di layar. Karena kemudahannya dan dapat membuka file teks dan menampilkannya di terminal teks saja, cat banyak digunakan hingga hari ini.
- Fitur ***more***, berarti dapat melihat file log secara lebih lengkap.
- Fitur ***less***, untuk menampilkan halaman di layer sebelumnya dan melihat layer berikutnya. Fitur ini juga dapat digunakan untuk melakukan pencarian *string.*
- Fitur ***tail***, digunakan untuk menampilkan sepuluh baris terakhir sebuah file teks.
- Fitur ***sudo***,Pada percobaan praktikum ini juga menggunakan fitur **sudo** atau *Super User Do* yang berfungsi untuk menjalankan task yang memerlukan izin administrative atau *root*. Maka dari itu jika menggunakan fitur ini kita perlu memasukkan *password for analyst*.

File log memiliki fungsi untuk memperkuat kemanan, yang mana data log menghubungkan peristiwa system atau jaringan yang akan menampilkan aktivitas pengguna. Teknisi sistem juga menggunakan *file* log untuk mengidentifikasi potensi masalah dan mencegah insiden. Kemudian jika terdapat kelebihan muatan server yang tak terduga berdampak negatif pada performa dan pengalaman pengguna. Sistem *file* log membantu melacak penggunaan sumber daya dan meningkatkan alokasi sumber daya. Dengan ini dapat membuat keputusan yang lebih baik terkait waktu untuk menaikkan atau menurunkan skala sumber daya.

Pertanyaan:

- Apa kelemahan menggunakan cat dengan file teks besar?
  Kelemahana cat adalah hanya akan menampilkan teks bagian akhirnya saja.

- Apa kelemahan menggunakan more?
  Kekurangan menggunakan perintah *more* adalah tidak dapat menampilkan teks dihalaman layer sebelumnya. Untuk menampilkan layer selanjutnya perlu menekan tombol *space* pada *keyboard*.

- Apa yang berbeda dalam output **tail** dan **tail -f**? Jelaskan!
  Pada percobaan ini tidak terlihat ada perbedaan output baik dengan perintah tail maupun tail -f.

- Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?
  Waktu dan tanggal yang tepat adalah kunci untuk analisis penyebab terjadinya masalah. Jika tidak sinkron maka akan sulit bagi administrator jaringan untuk menentukan urutan kejadian.

VI. KESIMPULAN

1. File Log adalah alat penting dalam pemecahan masalah dan pemantauan.
2. File log biasanya berisi informasi teks biasa yang dapat dilihat oleh hampir semua program yang dapat menangani teks.
3. Fungsi file log untuk mengidentifikasi masalah, meningkatkan operasi, meningkatkan efisiensi, memahami perilaku pengguna, memperkuat keamanan.
4. Syslog merupakan protokol standar yang dapat digunakan untuk mengirim log system.
5. Terdapat berbagai jenis perintah atau fitur yang dapat digunakan untuk menampilkan file teks.

DAFTAR PUSTAKA

Apa itu file log? (n.d.). Retrieved from aws.amazon: https://aws.amazon.com/id/what-is/log-files/#:~:text=Log%20server%20adalah%20file%20log,%2C%20jenis%20permintaan%2C%20dan%20sebagainya.

cnblogadmin. (2022, Oktober 27). *Syslog Server: Pengertian, Kegunaan dan Cara Installnya*. Retrieved Maret 12, 2023, from course-net: https://course-net.com/blog/syslog-server/

Putra, C. A. (2012, Desember 19). *Perintah Menampilkan file teks di Linux*. Retrieved Maret 13, 2023, from candra.web.id: https://www.candra.web.id/perintah-menampilkan-file-teks-di-linux/